

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
ESTADO-MAIOR DO EXÉRCITO

Separata ao Boletim do Exército

SEPARATA AO BE Nº 23/2017

ESTADO-MAIOR DO EXÉRCITO

PORTARIA Nº 222-EME, DE 5 DE JUNHO DE 2017.

Aprova a Metodologia da Política de Gestão de Riscos do Exército Brasileiro (EB20-D-07.089), 1ª Edição, 2017.

Brasília-DF, 9 de junho de 2017.



MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
ESTADO-MAIOR DO EXÉRCITO

PORTARIA Nº 222-EME, DE 5 DE JUNHO DE 2017.

Aprova a Metodologia da Política de Gestão de Riscos do Exército Brasileiro (EB20-D-07.089), 1ª Edição, 2017.

O **CHEFE DO ESTADO-MAIOR DO EXÉRCITO**, no uso das atribuições que lhe conferem a alínea g) do inciso I e o inciso IV do art. 4º do Regulamento do Estado-Maior do Exército (R-173), aprovado pela Portaria do Comandante do Exército nº 514, de 29 de junho de 2010, e de acordo com o que estabelece o artigo 44 das Instruções Gerais para as Publicações Padronizadas do Exército (EB10-IG-01.002), 1ª Edição, 2011, aprovadas pela Portaria do Comandante do Exército nº 770, de 7 de dezembro de 2011, ouvidos a Secretaria de Economia e Finanças (SEF) e o Centro de Controle Interno do Exército (CCIEx), resolve:

Art. 1º Instituir a Metodologia da Política de Gestão de Riscos do Exército Brasileiro (EB20-D-07.089), com a finalidade de:

I - orientar as Organizações Militares quanto à gestão de riscos e seus controles;

II - alinhar a gestão de riscos ao planejamento organizacional e estratégico;

III - otimizar o planejamento e a execução de programas, projetos e processos; e

IV - contribuir com a governança institucional.

Art. 2º Estabelecer que esta Portaria entre em vigor na data de sua publicação.

METODOLOGIA DA POLÍTICA DE GESTÃO DE RISCOS DO EXÉRCITO BRASILEIRO

ÍNDICE DE ASSUNTOS

Art.

PREFÁCIO

CAPÍTULO I - DOS CONCEITOS.......................................1º
CAPÍTULO II - DA CLASSIFICAÇÃO DOS RISCOS.......................................2º
CAPÍTULO III - DO PROCESSO DE GESTÃO DE RISCOS.......................................3º/4º
Seção I - Comunicação e consulta.......................................5º/9º
Seção II - Estabelecimento do contexto.......................................10
Subseção I - Estabelecimento do contexto externo.......................................11
Subseção II - Estabelecimento do contexto interno.......................................12/13
Subseção III - Estabelecimento do contexto do processo de gestão de riscos.......................................14/16
Seção III - Definição dos critérios de riscos.......................................17/19
Seção IV - Processo de avaliação de riscos.......................................20
Subseção I - Identificação de riscos.......................................21/29
Subseção II - Análise de riscos.......................................30/34
Subseção III - Avaliação de riscos.......................................35/40
Seção V - Tratamento de riscos.......................................41/46
Subseção I - Seleção das opções de tratamento de riscos.......................................47/49
Subseção II - Preparação e implementação de planos para tratamento de riscos.......................................50/55
Subseção III - Documentos de tratamento e controle de riscos.......................................56/60
Seção VI - Monitoramento e análise crítica.......................................61/65
CAPÍTULO IV - DAS DISPOSIÇÕES FINAIS.......................................66/70
REFERÊNCIAS
ANEXOS

PREFÁCIO

A filosofia de gestão de riscos do Exército é representada pelo conjunto de convicções e atitudes compartilhadas que caracterizam a forma pela qual a Instituição considera o risco em tudo aquilo que faz, do desenvolvimento e da implementação de estratégias às suas atividades do dia-a-dia. Sua filosofia de gestão de riscos reflete em seus valores, influencia a sua cultura e seu estilo operacional, bem como afeta a forma com que os componentes de gestão de riscos são aplicados, inclusive como os riscos são identificados, os tipos de riscos que são aceitáveis e a forma pela qual são administrados.

O Comitê de Governança, Riscos e Controles do Exército representa uma parte crítica do ambiente interno e é capaz de influenciar os seus elementos de forma significativa. A despeito do fato que, historicamente, uma instituição não tenha incorrido em prejuízos e nem se exponha muito a riscos, os membros do Comitê não devem sucumbir à noção mítica de que eventos que trazem sérias consequências adversas não vão ocorrer no Exército. Eles reconhecem que, embora a Instituição possa ter uma estratégia perfeita, pessoas competentes, processos íntegros e tecnologia confiável, ela, como qualquer outra instituição, é vulnerável a risco e necessita de uma gestão de riscos eficaz.

Cabe destacar que as estratégias e os objetivos do Exército e o modo pelo qual são implementados baseiam-se em preferências, julgamentos de valor e estilos gerenciais. A integridade e o compromisso da Alta Administração com valores éticos influenciam estas preferências e estes julgamentos, os quais são traduzidos em normas de comportamento. Assim, a boa reputação da Instituição, por ser tão valiosa, faz com que seus padrões de comportamento se estendam para além do mero cumprimento de normas.

Ressalta-se, ainda, que a competência profissional dos militares e civis do Exército reflete no conhecimento e nas habilidades necessárias à execução das tarefas designadas. A Alta Administração do Exército decide quão bem estas tarefas necessitam ser executadas, ponderando as estratégias e os objetivos da Instituição, bem como os planos para a sua implementação e realização. A Alta Administração do Exército estipula os níveis de competência para determinados trabalhos e traduz esses níveis em habilidades e conhecimentos necessários, que por sua vez, podem depender do grau de inteligência, treinamento e experiência individual. Os fatores considerados no desenvolvimento dos níveis de conhecimentos e habilidades incluem a natureza e o grau de julgamento utilizado em uma função específica.

Desse modo, a estrutura organizacional do Exército provê o arcabouço para planejar, executar, controlar e monitorar as suas atividades. A estrutura inclui a definição de áreas fundamentais de autoridade e responsabilidade, bem como a definição de linhas apropriadas de comunicação. A atribuição de alçada e responsabilidade inclui até que ponto pessoas e equipes estão autorizadas e são incentivadas a adotar sua própria iniciativa ao abordar questões, bem como a solucionar problemas e os limites desta autoridade. A delegação de autoridade significa passar o controle central de determinadas decisões aos escalões inferiores, ou seja, para o pessoal que está mais próximo das atividades cotidianas.

Nesse contexto, o desafio crucial é delegar apenas até o grau necessário ao alcance dos objetivos, a fim de assegurar que o processo decisório esteja embasado em práticas sadias de identificação e avaliação de riscos, inclusive o dimensionamento de riscos e a comparação entre o potencial de prejuízo com os ganhos na determinação de quais riscos aceitar e de como serão administrados. Outro desafio é assegurar que todo o pessoal entenda os objetivos da Instituição.

Portanto, é essencial que as pessoas compreendam de que forma suas ações se inter-relacionam e contribuem para a realização dos objetivos.

CAPÍTULO I
DOS CONCEITOS

Art. 1º Para fins conceituais desta Metodologia da Política de Gestão de Riscos do Exército Brasileiro, em ordem lógica, considera-se:

I - *accountability*: conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações;

II - auditoria interna: atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia a organização a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, de controles internos, de integridade e de governança. As auditorias internas no âmbito da Administração Pública se constituem na terceira linha ou camada de defesa das organizações, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa, executada por todos os níveis de gestão dentro da organização) e da supervisão dos controles internos (segunda linha ou camada de defesa, executada por instâncias específicas, como comitês de risco e controles internos);

III - governança: combinação de processos e estruturas implantadas pela Alta Administração para informar, dirigir, administrar e monitorar as atividades da organização, com o intuito de alcançar seus objetivos;

IV - governança no setor público: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

V - gerenciamento de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização;

VI - evento: ocorrência ou alteração em um conjunto específico de circunstâncias capaz de causar impacto na implementação da estratégia ou na realização de objetivos;

Nota 1: um evento pode consistir em uma ou mais ocorrências e pode ter várias causas;

Nota 2: um evento pode consistir em alguma coisa não acontecer;

Nota 3: um evento pode, algumas vezes, ser referido como um "incidente" ou um "acidente".

VII - incerteza: incapacidade de saber, com antecedência, a real probabilidade ou impacto de eventos futuros;

VIII - risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade. O risco é o efeito da incerteza sobre os objetivos. Um efeito é um desvio em relação ao esperado, podendo ser positivo (oportunidade) ou negativo (ameaça);

Nota 1: oportunidades são características externas não controláveis com potencial para melhorar o desempenho;

Nota 2: ameaças são características externas não controláveis que podem comprometer o desempenho.

IX - causas de risco ou fatores de risco: são as condições que podem dar origem à possibilidade de um evento acontecer. Podem ter origem no ambiente interno ou externo. Relacionam as fontes de risco e suas vulnerabilidades. Exemplos: processos mal concebidos ou sistemas informatizados obsoletos;

Nota 1: fontes de risco são os elementos que, individualmente ou combinados, têm o potencial intrínseco para dar origem ao risco, podendo ser tangíveis ou intangíveis;

Nota 2: vulnerabilidades são inexistências, inadequações ou deficiências em uma fonte de risco.

X - consequências do risco: é o resultado de um evento sobre os objetivos;

XI - risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

XII - risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

XIII - mensuração de risco: significa estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência;

XIV - tolerância a riscos: faixa de desvios em relação aos níveis de riscos determinados como aceitáveis por uma organização durante o desempenho de suas operações;

XV - apetite a riscos: grau de exposição aos riscos que a organização está disposta a aceitar para atingir seus objetivos e criar valor;

XVI - fraude: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência ou de força física. Fraude é um tipo específico de risco;

XVII - gestor (proprietário) do risco: pessoa ou entidade com a responsabilidade e autoridade para gerenciar um risco;

XVIII - gestão integrada de riscos: arquitetura implantada internamente na organização para gerenciar os riscos de maneira eficaz, contribuindo para a redução da materialização de eventos que impactem negativamente seus objetivos. A gestão integrada de riscos, através de um enfoque estruturado e da melhor compreensão das inter-relações entre riscos, alinha estratégia, processos, pessoas, tecnologia e conhecimentos, objetivando a preservação e a criação de valor para a organização;

XIX - plano de gestão de riscos: esquema dentro da estrutura da gestão de riscos, que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos;

Nota 1: os componentes de gestão tipicamente incluem procedimentos, práticas, atribuição de responsabilidades, sequência e cronologia das atividades;

Nota 2: o plano de gestão de riscos pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização ou seu componente.

XX - Portfólio de Riscos Prioritários: grupo de riscos com impacto potencialmente elevado para o negócio, cuja gestão deve ser priorizada e os seus indicadores e metas devem ser monitorados regularmente;

XXI - monitoramento: é obtido por meio de revisões específicas ou monitoramento contínuo (independente ou não), realizados sobre todos os demais componentes de controles internos, com o fim de aferir sua eficácia, eficiência, efetividade, economicidade, excelência ou execução na implementação dos seus componentes e corrigir tempestivamente as deficiências dos controles internos;

XXII - monitoramento contínuo: é realizado nas operações normais e de natureza contínua da organização. Inclui a administração e as atividades de supervisão e outras ações que os servidores executam ao cumprir suas responsabilidades. Abrange cada um dos componentes da estrutura do controle interno, fortalecendo os controles internos da gestão contra ações irregulares, antiéticas, antieconômicas, ineficientes e ineficazes. Pode ser realizado pela própria Administração por intermédio de instâncias de conformidade, como comitês específicos, que atuam como segunda linha (ou camada) de defesa da organização;

XXIII - avaliações específicas: são realizadas com base em métodos e procedimentos predefinidos, cuja abrangência e frequência dependerão da avaliação de risco e da eficácia dos procedimentos de monitoramento contínuo. Abrangem, também, a avaliação realizada pelas unidades de auditoria interna dos Órgãos e entidades e pelos Órgãos do Sistema de Controle Interno do Poder Executivo federal para aferição da eficácia dos controles internos da gestão quanto ao alcance dos resultados desejados;

XXIV - Sistema de Controle Interno do Poder Executivo federal: compreende as atividades de avaliação do cumprimento das metas previstas no plano plurianual, da execução dos programas de governo e dos orçamentos da União e de avaliação da gestão dos administradores públicos federais, utilizando como instrumentos a auditoria e a fiscalização, e tendo como Órgão central a Controladoria-Geral da União. Não se confunde com os controles internos da gestão, de responsabilidade de cada Órgão e entidade do Poder Executivo federal;

XXV - estrutura da gestão de riscos: conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização;

Nota 1: os fundamentos incluem a política, objetivos, mandatos e comprometimento para gerenciar riscos;

Nota 2: os arranjos organizacionais incluem planos, relacionamentos, responsabilidades, recursos, processos e atividades;

Nota 3: a estrutura da gestão de riscos está incorporada no âmbito das normas e práticas estratégicas e operacionais de toda a organização.

XXVI - responsabilização: a organização deve assegurar que haja responsabilização, autoridade e competência apropriadas para gerenciar riscos, incluindo implementar e manter o processo de gestão de riscos e assegurar a suficiência, a eficácia e a eficiência de quaisquer controles. Isto pode ser facilitado por:

a) identificação dos proprietários dos riscos que têm a responsabilidade e a autoridade para gerenciar riscos;

b) identificação dos responsáveis pelo desenvolvimento, implementação e manutenção da estrutura para gerenciar riscos;

c) identificação de outras responsabilidades das pessoas, em todos os níveis da organização, no processo de gestão de riscos;

d) estabelecimento da medição de desempenho e processos de reporte internos ou externos e relação com os devidos escalões; e

e) estabelecimento de níveis apropriados de reconhecimento;

XXVII - controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão, os seguintes objetivos gerais serão alcançados:

a) execução ordenada, ética, econômica, eficiente e eficaz das operações;

b) cumprimento das obrigações de *accountability*;

c) cumprimento das leis e regulamentos aplicáveis; e

d) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente a aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados de forma eficaz, eficiente, efetiva e econômica;

XXVIII - <u>5W2H</u> é uma ferramenta cujos sete caracteres correspondem às iniciais (em inglês) das diretrizes que, quando bem estabelecidas, eliminam quaisquer dúvidas que possam aparecer ao longo de um processo ou de uma atividade. São elas: *5W: What* (o que será feito?), *Why* (por que será feito?), *Where* (onde será feito?), *When* (quando?), *Who* (por quem será feito?); *2H: How* (como será feito?), *How much* (quanto vai custar?).

CAPÍTULO II
DA CLASSIFICAÇÃO DOS RISCOS

Art. 2º Para fins de adoção desta Metodologia de Gestão de Riscos, estes são classificados da seguinte forma:

I - Riscos Estratégicos: eventos que podem impedir ou afetar o atingimento das decisões estratégicas do Alto Comando do Exército, definidas em seu Plano Estratégico e outros documentos.

Neste contexto, inserem-se as decisões sobre programas e projetos, tanto a cargo do Estado-Maior do Exército como dos Órgãos setoriais;

II - Riscos Operacionais: eventos que podem comprometer os objetivos e as atividades das Organizações Militares, normalmente associadas a falhas, deficiências ou inadequação de processos internos, pessoas, infraestruturas e sistemas. Inclue-se, também, a possibilidade de ocorrência de eventos críticos em exercícios e em operações militares;

III - Riscos de Imagem/Reputação: eventos que podem comprometer a confiança da sociedade em relação à capacidade da Força Terrestre ou de qualquer uma de suas Organizações Militares em bem cumprir sua missão regulamentar;

IV - Riscos de Conformidade: eventos relacionados à falta de habilidade ou disciplina da Organização Militar para cumprir com a legislação e/ou regulamentação externa e às normas e procedimentos internos. Por incluir as normas e procedimentos internos, apresenta um contexto mais amplo do que o tipo de risco mais usualmente citado, o risco legal/regulatório, decorrente da aplicação da legislação trabalhista, tributária, fiscal, referentes a relações contratuais, regulamentação de mercado e de prestação de serviços;

V - Riscos Financeiros/Orçamentários: eventos que podem comprometer a capacidade da Organização Militar de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações ou contingenciamento de recursos;

VI - Riscos Tecnológicos: eventos representados por falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da Organização Militar, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais). Pode estar também associado a erros ou fraudes, internas ou externas, nos sistemas informatizados ao capturar, registrar, monitorar e reportar incorretamente transações ou posições;

VII - Riscos de Segurança da Informação: eventos ligados à possibilidade de determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos (recursos humanos, informação, material e áreas e instalações), desta maneira prejudicando a Organização Militar; e

VIII - Riscos ao Meio Ambiente: eventos associados à gestão inadequada de questões ambientais, causando efeitos como contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos.

Parágrafo único. Poderão existir outros riscos, se necessário, caso seja considerado não haver um único tipo de classificação de riscos que seja consensual, exaustivo e aplicável a todas as organizações. Assim, a classificação deve ser utilizada de acordo com as características de cada Organização Militar, contemplando suas peculiaridades.

CAPÍTULO III
DO PROCESSO DE GESTÃO DE RISCOS

Art. 3º A gestão de riscos deve ser aplicada a toda Organização Militar, em suas várias áreas e níveis, a qualquer momento, bem como a funções, atividades e projetos específicos.

Art. 4º O processo de gestão de riscos auxilia a tomada de decisão, levando em consideração as incertezas e a possibilidade de circunstâncias ou eventos futuros (intencionais ou não intencionais) e seus efeitos sobre os objetivos acordados. A definição das partes do processo de gestão de riscos tem a seguinte configuração:

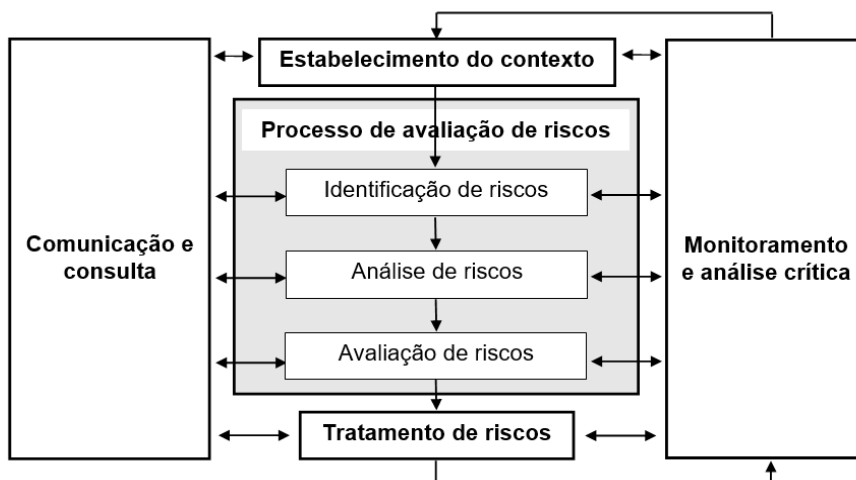


Figura 1 - processo de gestão de riscos

Seção I
Comunicação e consulta

Art. 5º A comunicação e a consulta às partes interessadas internas e externas devem acontecer durante todas as fases do processo de gestão de riscos. Portanto, os planos e critérios de comunicação e consulta devem ser desenvolvidos em um estágio inicial.

Art. 6º Estes planos devem abordar questões relacionadas com o risco propriamente dito, suas causas, suas consequências (se conhecidas) e as medidas que estão sendo tomadas para tratá-los.

Art. 7º A comunicação e consulta interna e externa eficazes são realizadas com a finalidade de assegurar que os responsáveis pela implementação do processo de gestão de riscos e as partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as razões pelas quais ações específicas são requeridas.

Art. 8º A comunicação e consulta às partes interessadas são importantes na medida em que elas fazem julgamentos sobre riscos com base em suas percepções, que podem variar devido às diferenças de valores, necessidades, suposições, conceitos e preocupações das partes interessadas. Como os seus pontos de vista podem ter um impacto significativo sobre as decisões tomadas, convém que as percepções das partes interessadas sejam identificadas, registradas e levadas em consideração no processo de tomada de decisão.

Art. 9º A comunicação e a consulta devem facilitar a troca de informações verdadeiras, pertinentes, exatas e compreensíveis, levando em consideração os aspectos de confidencialidade e integridade das pessoas.

Seção II
Estabelecimento do contexto

Art. 10. Ao estabelecer o contexto, a organização articula seus objetivos, define os parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelece o escopo e os critérios de risco para o restante do processo.

Parágrafo único. Mesmo que muitos destes parâmetros sejam similares àqueles considerados na concepção da estrutura da gestão de riscos, eles precisam ser considerados com mais detalhe e, em particular, como eles se relacionam com o escopo do respectivo processo de gestão de riscos.

Subseção I
Estabelecimento do contexto externo

Art. 11. O contexto externo é o ambiente externo no qual a organização busca atingir seus objetivos.

§ 1º Os objetivos e as preocupações das partes interessadas externas devem ser considerados no desenvolvimento dos critérios de risco.

§ 2º O contexto externo pode incluir, mas não está limitado a:

I - ambientes cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, quer seja internacional, nacional, regional ou local;

II - fatores-chave e tendências que tenham impacto sobre os objetivos da organização; e

III - relações com as partes interessadas externas e suas percepções e valores.

Subseção II
Estabelecimento do contexto interno

Art. 12. O contexto interno é o ambiente interno no qual a organização busca atingir seus objetivos.

§ 1º O processo de gestão de riscos deve estar alinhado com a cultura, processos, estrutura e estratégias da organização. O contexto interno é algo dentro da organização que pode influenciar a maneira pela qual uma organização gerenciará os riscos.

§ 2º Convém que ele seja estabelecido, porque:

I - a gestão de riscos ocorre no contexto dos objetivos da organização;

II - é importante que os objetivos e os critérios de um determinado projeto, processo ou atividade sejam considerados tendo como base os objetivos da organização como um todo; e

III - algumas organizações deixam de reconhecer oportunidades para atingir seus objetivos estratégicos, de projeto ou de negócios, o que afeta o comprometimento, a credibilidade, a confiança e o valor organizacional.

Art. 13. É necessário compreender o contexto interno. Isto pode incluir, mas não está limitado a:

I - governança, estrutura organizacional, funções e responsabilidades;

II - políticas, objetivos e estratégias implementadas para atingi-los;

III - capacidades, entendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);

IV - sistemas de informação, fluxos de informação e processos de tomada de decisão (formais e informais);

V - relações com as partes interessadas internas e suas percepções e valores;

VI - cultura da organização;

VII - normas, diretrizes e modelos adotados pela organização; e

VIII - forma e extensão das relações contratuais.

Subseção III
Estabelecimento do contexto do processo de gestão de riscos

Art. 14. Devem ser estabelecidos os objetivos, as estratégias, o escopo e os parâmetros das atividades da organização, ou daquelas partes da organização em que o processo de gestão de riscos está sendo aplicado.

Art. 15. A gestão dos riscos deve ser realizada com plena consciência da necessidade de justificar os recursos utilizados na gestão de riscos. Convém ainda que os recursos requeridos, as responsabilidades e as autoridades, além dos registros a serem mantidos, também sejam especificados.

Art. 16. O contexto do processo de gestão de riscos irá variar de acordo com as necessidades de uma organização. Ele pode envolver, mas não está limitado a:

I - definição das metas e objetivos das atividades de gestão de riscos;

II - definição das responsabilidades pelo processo e dentro da gestão de riscos;

III - definição do escopo, bem como da profundidade e da amplitude das atividades da gestão de riscos a serem realizadas, englobando inclusões e exclusões específicas;

IV - definição da atividade, processo, função, projeto, produto, serviço ou ativo em termos de tempo e localização;

V - definição das relações entre um projeto, processo ou atividade específicos e outros projetos, processos ou atividades da organização;

VI - definição das metodologias de processo de avaliação de riscos;

VII - definição da forma como são avaliados o desempenho e a eficácia na gestão dos riscos;

VIII - identificação e especificação das decisões que têm que ser tomadas; e

IX - identificação, definição ou elaboração dos estudos necessários, de sua extensão e objetivos, e dos recursos requeridos para tais estudos.

Parágrafo único. A atenção para estes e outros fatores pertinentes pode ajudar a assegurar que a abordagem adotada para a gestão de riscos seja apropriada às circunstâncias, à organização e aos riscos que afetam a realização de seus objetivos.

Seção III
Definição dos critérios de riscos

Art. 17. A organização deve definir os critérios a serem utilizados para avaliar a significância do risco, a fim de refletirem os valores, objetivos e recursos da organização. Alguns critérios podem ser impostos por (ou derivados de) requisitos legais e regulatórios e outros requisitos que a organização subscreva.

Art. 18. Os critérios de risco devem ser compatíveis com a política de gestão de riscos da organização, definidos no início de qualquer processo de gestão de riscos e analisados criticamente de forma contínua.

Art. 19. Ao definir os critérios de riscos, convém que os fatores a serem considerados incluam os seguintes aspectos:

I - a natureza e os tipos de causas e de consequências que podem ocorrer e como elas serão medidas;

II - como a probabilidade será definida;

III - a evolução no tempo da probabilidade e/ou consequência(s);

IV - como o nível de risco deve ser determinado;

V - os pontos de vista das partes interessadas;

VI - o nível em que o risco se torna aceitável ou tolerável; e

VII - se convém que combinações de múltiplos riscos sejam levadas em consideração e, em caso afirmativo, como e quais combinações convém que sejam consideradas.

Seção IV
Processo de avaliação de riscos

Art. 20. O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos.

Subseção I
Identificação de riscos

Art. 21. A organização deve identificar as fontes de risco, eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências potenciais. A finalidade desta etapa é gerar uma lista

abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos.

Parágrafo único. Uma identificação abrangente é crítica, pois um risco que não for identificado nesta fase não será incluído em análises posteriores.

Art. 22. A identificação deve incluir todos os riscos, estando suas fontes sob o controle da organização ou não, mesmo que as fontes ou causas dos riscos possam não ser evidentes.

Art. 23. A identificação de riscos deve incluir o exame de reações em cadeia provocadas por consequências específicas, incluindo os efeitos cumulativos e em cascata.

Art. 24. Uma ampla gama de consequências deve ser considerada, mesmo que a fonte ou causa do risco não estejam evidentes. Além de identificar o que pode acontecer, é necessário considerar possíveis causas e cenários que mostrem quais consequências podem ocorrer.

Art. 25. A organização deve aplicar ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos, considerando que informações pertinentes e atualizadas são importantes na identificação de riscos.

Art. 26. Pessoas com um conhecimento adequado podem ser envolvidas na identificação dos riscos e todas as causas e consequências significativas devem ser consideradas.

Art. 27. Para a identificação de riscos, recomenda-se a utilização dos processos listados na Norma ABNT ISO 31010, como o *Brainstorming*, técnica SWIFT, método *Delphi* e a matriz de probabilidade/consequência.

Art. 28. Em suma, a identificação dos riscos consiste em desenhar uma matriz, conforme modelo a seguir, sempre considerando o ambiente externo e interno (análise SWOT), bem como definindo antes a situação do evento, se incerteza ou risco.

Dados / **Categorias**	**Objetivos ou processos**	**Fatores Críticos de Sucesso**	**Riscos**	**Causas potenciais**	**Consequências potenciais**
1. Estratégicos			1.1 ALFA		
			1.2 BRAVO		
			...		
2. Operacionais			2.1 DELTA		
			2.2 ECHO		
			...		
3. De imagem/ Reputação			3.1 HOTEL		
			3.2 INDIA		
			...		
4. De Conformidade			4.1 JULIET		
			4.2 KILO		
			...		
5. Financeiros/ Orçamentários			5.1 LIMA		
			5.2 MIKE		
			...		

Dados / Categorias	Objetivos ou processos	Fatores Críticos de Sucesso	Riscos	Causas potenciais	Consequências potenciais
6. Tecnológicos			6.1 OSCAR		
			6.2 PAPA		
			...		
7. De Segurança da Informação			7.1 QUEBEC		
			7.2 ROMEO		
			...		
8. Ao Meio Ambiente			8.1 SIERRA		
			8.2 TANGO		
			...		
9. Outros			...		

Quadro 1 - Matriz de identificação de riscos (modelo)

§ 1º Para o preenchimento da coluna categorias, os programas e projetos devem utilizar as respectivas áreas do conhecimento, previstas no Guia de Conhecimento sobre Gerenciamento de Projetos (PMBOK, sigla em inglês; 5ª edição), e conforme as Normas de Elaboração, Gerenciamento e Acompanhamento de Projetos no Exército Brasileiro (NEGAPEB) e as Normas de Elaboração, Gerenciamento e Acompanhamento do Portfólio e dos Programas Estratégicos do Exército Brasileiro (NEGAPORT).

§ 2º As Seções e Repartições das Organizações Militares elaboram suas Matrizes de Identificação de Riscos com base em seus processos.

§ 3º Uma Organização Militar que tenha 15 objetivos poderá chegar, em média, a 180 riscos mapeados (15 objetivos x 3 fatores críticos de sucesso x 4 riscos). A média geral é de 10 a 15 riscos por objetivo.

Art. 29. As Organizações Militares deverão listar em suas Matrizes de Identificação de Riscos, se possível, pelo menos 1 (um) risco nas seguintes áreas: Operacional, Reputação/imagem, Conformidade, Financeiro/Orçamentário e de Segurança da Informação, com base nos seus objetivos, previstos no Plano de Gestão.

Subseção II
Análise de riscos

Art. 30. A análise de riscos visa a promover o entendimento do nível de risco e de sua natureza, auxiliando na definição de prioridades e opções de tratamento aos riscos identificados. Por meio dela, é possível saber qual a probabilidade de os riscos virem a acontecer e calcular seus respectivos impactos nos objetivos, projetos e processos organizacionais.

Art. 31. Os riscos são analisados de maneira qualitativa (subjetiva), ou seja, utiliza-se critérios preestabelecidos com uma escala de valoração para a determinação do nível do risco, visto que a metodologia a ser utilizada para a avaliação de riscos (passo seguinte) possui dois parâmetros claros a serem analisados:

I - saber qual a probabilidade dos riscos virem a acontecer, frente à condição existente de cada objetivo, projeto ou processo; e

II - calcular o impacto, caso o risco ocorra.

Art. 32. Os termos relacionados à probabilidade de riscos são assim descritos em termos qualitativos:

NÍVEL	VALOR	DESCRIÇÃO
1	MUITO BAIXA	Evento extraordinário para os padrões conhecidos da gestão e operação do processo. Embora possa assumir dimensão estratégica para a manutenção do processo, não há histórico disponível de sua ocorrência.
2	BAIXA	Evento casual, inesperado. Muito embora raro, há histórico de sua ocorrência por parte dos principais gestores e operadores do processo.
3	MÉDIA	Evento esperado, que se reproduz com frequência reduzida, porém constante. Seu histórico de ocorrência é de conhecimento da maioria dos gestores e operadores do processo.
4	ALTA	Evento usual, corriqueiro. Devido à sua ocorrência habitual ou conhecida em uma dezena ou mais de casos, aproximadamente, seu histórico é amplamente conhecido por parte de gestores e operadores do processo.
5	MUITO ALTA	Evento se reproduz muitas vezes, se repete seguidamente, de maneira assídua, numerosa e, não raro, de modo acelerado. Interfere de modo claro no ritmo das atividades, sendo evidente para os que conhecem o processo.

Quadro 2 - Avaliação qualitativa de probabilidade

Art. 33. Os termos relacionados ao impacto de riscos são descritos em termos qualitativos como:

NÍVEL	VALOR	DESCRIÇÃO
1	MUITO BAIXO	Degradação de operações, atividades, projetos, programas ou processos da organização, porém causando impactos mínimos nos objetivos (de tempo, prazo, custo, quantidade, qualidade, acesso, escopo, imagem etc) relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas (clientes internos e externos, beneficiários).
2	BAIXO	Degradação de operações, atividades, projetos, programas ou processos da organização, causando impactos pequenos nos objetivos.
3	MÉDIO	Interrupção de operações, atividades, projetos, programas ou processos da organização, causando impactos significativos nos objetivos, porém recuperáveis.
4	ALTO	Interrupção de operações, atividades, projetos, programas ou processos da organização, causando impactos de reversão muito difícil nos objetivos.
5	MUITO ALTO	Interrupção abrupta de operações, atividades, projetos, programas ou processos da organização, influenciando fortemente outros processos e causando impactos nos objetivos de dificílima reversão.

Quadro 3 - Avaliação qualitativa de impacto

Art. 34. Com base na construção da tabela (hipotética), a seguir, serão levantados todos os riscos da organização, inclusive por seus setores subordinados.

RISCOS	PROBABILIDADE (P) (1 a 5)	IMPACTO (I) (1 a 5)
1.1 ALFA	2	5
1.2 BRAVO	2	3
1.3 CHARLIE	4	4
2.1 DELTA	4	3
2.2 ECHO	3	5

RISCOS	PROBABILIDADE (P) (1 a 5)	IMPACTO (I) (1 a 5)
2.3 FOXTROT	2	2
2.4 GOLF	1	2
....	...	...
n		

Quadro 4 - Matriz de exposição a riscos (probabilidade x impacto) (exemplo)

§ 1º Ao final dessa etapa, os riscos estarão todos listados e devidamente identificados quanto à probabilidade e impacto, ocasião em que se poderá, ainda, fazer os devidos ajustes para mais ou para menos.

§ 2º Alguns riscos podem ser agrupados em uma única descrição.

Subseção III
Avaliação de riscos

Art. 35. A finalidade da avaliação de riscos é auxiliar na tomada de decisão com base nos resultados da análise daqueles que necessitam de tratamento, bem como a prioridade para sua implementação.

Art. 36. A relevância dos riscos possui, como parâmetro, a matriz de exposição a riscos, e o seu resultado é o grau de criticidade do risco, ou seja, é a priorização que o setor responsável deve utilizar para tratar cada risco, frente ao apetite a riscos.

Art. 37. A matriz de exposição a riscos demonstra os pontos de cruzamento (horizontal e vertical) da probabilidade de ocorrência e do impacto. Essas duas dimensões de risco, quando combinadas, resultam em um terceiro elemento de risco denominado nível de risco.

Art. 38. A parametrização dos níveis de risco, mediante a combinação das dimensões probabilidade x impacto foi arbitrada como se segue:

I - área vermelha: os riscos existentes são aqueles que têm alta probabilidade de ocorrência e poderão resultar em impacto extremamente severo, caso ocorram. Exigem a implementação imediata das ações de proteção e prevenção;

II - área laranja: onde se localizam as ameaças que poderão ser muito danosas à organização, podendo possuir muito baixa probabilidade e alto impacto, bem como baixo impacto e alta probabilidade. Estas ameaças devem possuir respostas rápidas que, para isso, devem estar planejadas e testadas em um plano de contingência, além de ações preventivas. São eventos que devem ser constantemente monitorados;

III - área amarela: nesta área estão os riscos com alta probabilidade de ocorrência, mas que possuem consequências gerenciáveis à organização. Os riscos classificados neste quadrante devem ser monitorados de forma rotineira e sistemática, podendo também possuir planos de contingência, se for o caso; e

IV - área verde: nesta área estão os riscos que possuem baixa probabilidade e pequeno impacto, representando pequenos problemas e prejuízos. Estes riscos somente devem ser gerenciados e administrados, pois, em princípio, estão em zona de conforto.

IMPACTO						
	5 MUITO ALTO	5	10	15	20 EXTREMO	25
	4 ALTO	4	8	12	16	20
	3 MÉDIO	3	6	9 ALTO	12	15
	2 BAIXO	2	4 MÉDIO	6	8	10
	1 MUITO BAIXO	1 BAIXO	2	3	4	5
Classificação de riscos: - EXTREMO - ALTO - MÉDIO - BAIXO		1 MUITO BAIXA	2 BAIXA	3 MÉDIA	4 ALTA	5 MUITO ALTA
		PROBABILIDADE				

Quadro 5 - Matriz de classificação de exposição a riscos (probabilidade x impacto)

Parágrafo único. Do produto da prioridade x impacto do caso hipotético e de sua análise, obtém-se a criticidade dos riscos, conforme modelo a seguir.

RISCOS	PROBABILIDADE (P) (1 A 5)	IMPACTO (I) (1 A 5)	NÍVEL DE RISCO P X I = ...	CRITICIDADE (O Prio)
1.1 ALFA	2	5	10	4º
1.2 BRAVO	2	3	06	5º
1.3 CHARLIE	4	4	16	1º
2.1 DELTA	4	3	12	3º
2.2 ECHO	3	5	15	2º
2.3 FOXTROT	2	2	04	6º
2.4 GOLF	1	2	02	7º
....	...	...	...	...

Quadro 6 - Matriz de criticidade de riscos (exemplo)

Art. 39. A classificação dos níveis de riscos e suas providências são assim definidas:

TIPO	ÁREA	PONTUAÇÃO	PROVIDÊNCIAS
EXTREMO	vermelha	15 a 25	ação imediata
ALTO	laranja	8 a 12	ação média e no curto prazo
MÉDIO	amarela	3 a 6	monitoramento e gestão
BAIXO	verde	1 a 2	risco controlável

Quadro 7 - Pontuação por classificação de risco

Art. 40. O processo de gestão de riscos permite à organização obter uma priorização dos riscos, conforme a seguir, que favorecerá a tomada de decisão e a boa gestão de recursos empregados.

CRITICIDADE (O Prio)	**CÓDIGO DO RISCO**	**RISCOS**	**VALOR DO RISCO**	**CLASSIFICAÇÃO DO NÍVEL DE RISCO**
1º	R1	CHARLIE	16	EXTREMO*
2º	R2	ECHO	15	EXTREMO*
3º	R3	DELTA	12	ALTO*
4º	R4	ALFA	10	ALTO*
5º	R5	BRAVO	06	MÉDIO
6º	R6	FOXTROT	04	MÉDIO
7º	R7	GOLF	02	BAIXO
...	....	....	...	...

* Os riscos extremos e altos devem, se possível, ser tratados, a fim de se obter uma classificação que dê maior segurança à Organização Militar.

Quadro 8 - Matriz de priorização de riscos (exemplo)

Parágrafo único. Nesta ocasião, os riscos serão codificados, a fim de facilitar o seu monitoramento e controle ao longo do tempo, inclusive quanto às possíveis mudanças de sua ordem de prioridade.

Seção V
Tratamento de riscos

Art. 41. O tratamento de riscos envolve a seleção de uma ou mais opções para modifica-los e a implementação dessas opções, de acordo com o que foi priorizado. Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes.

Art. 42. Tratar riscos envolve um processo cíclico, composto por:

I - avaliação do tratamento de riscos já realizado;

II - decisão se os níveis de risco residual são toleráveis; se não forem toleráveis, a definição e implementação de um novo tratamento para os riscos; e

III - avaliação da eficácia deste tratamento.

Art. 43. Os tomadores de decisão são os responsáveis pela implantação da resposta ou tratamento dos riscos. Ou seja, com o uso da matriz de priorização de riscos, deve-se identificar qual a resposta a ser dada para o tratamento do risco.

Art. 44. São estas as respostas a riscos que podem ser adotadas:

I - evitar o risco: decisão de não se envolver ou agir de forma a se retirar de uma situação de risco. Nem sempre é possível se dar essa resposta, o que obriga a realmente tratar o risco, reduzindo-o;

II - aceitar e reter: manter o risco no nível atual de impacto e probabilidade;

III - aceitar e reduzir/mitigar: ações são tomadas para minimizar a probabilidade e/ou impacto do risco; e

IV - aceitar e transferir e/ou compartilhar o risco: atividades que visam reduzir o impacto e/ou a probabilidade de ocorrência do risco por meio da transferência ou, em alguns casos, do compartilhamento de uma parte do risco.

Art. 45. O risco é assumido quando o Comandante, Chefe ou Diretor decide admitir risco na área de risco alto (8 a 12 pontos), visto que não são aceitáveis riscos extremos, exceto se autorizado pelo Comitê de Governança, Riscos e Controles do Exército.

§ 1º Se por ocasião da análise inicial dos riscos algum destes for classificado na área de risco extremo, deve-se elaborar um plano de tratamento de riscos para levá-lo para a área de risco alto ou médio.

§ 2º Se mesmo assim não for possível, deve-se evita-lo ou solicitar autorização ao escalão superior para se correr este risco, seguindo-se o previsto no Capítulo VIII da Política de Gestão de Riscos do Exército.

Art. 46. Sempre que houver a necessidade de tratamento de um risco, deve-se considerar a equação custo x benefício, a fim de se saber se o tratamento não tem custo superior à hipótese de se correr determinado risco.

Subseção I
Seleção das opções de tratamento de riscos

Art. 47. Selecionar a opção mais adequada de tratamento de riscos envolve equilibrar, de um lado, os custos e os esforços de implementação e, de outro, os benefícios decorrentes, relativos a requisitos legais, regulatórios ou quaisquer outros, tais como o da responsabilidade social e o da proteção do ambiente natural.

Art. 48. As decisões também devem levar em consideração os riscos que demandam um tratamento economicamente não justificável, como, por exemplo, riscos severos (com grande consequência negativa), porém raros (com probabilidade muito baixa).

Art. 49. Várias opções de tratamento podem ser consideradas e aplicadas individualmente ou combinadas. A organização, normalmente, beneficia-se com a adoção de uma combinação de opções de tratamento.

§ 1º Ao selecionar as opções de tratamento de riscos, a organização deve considerar os valores e as percepções das partes interessadas e as formas mais adequadas para se comunicar com elas.

§ 2º Quando as opções de tratamento de riscos podem afetar o risco no restante da organização ou às partes interessadas, é importante que todos os envolvidos participem da decisão. Embora igualmente eficazes, alguns tratamentos podem ser mais aceitáveis para algumas das partes interessadas do que para outras.

Subseção II
Preparação e implementação de planos para tratamento de riscos

Art. 50. A finalidade dos planos de tratamento de riscos é documentar como as opções de tratamento escolhidas serão implementadas.

Art. 51. As informações fornecidas nos planos de tratamento devem incluir:

I - as razões para a seleção das opções de tratamento, inclusive os benefícios que se espera obter;

II - os responsáveis pela aprovação do plano e os responsáveis pela sua implementação;

III - ações propostas;

IV - os recursos requeridos, incluindo ações de contingências;

V - medidas de desempenho e restrições;

VI - requisitos para a apresentação de informações e de monitoramento; e

VII - cronograma e programação.

Art. 52. Os planos de tratamento devem ser integrados com os processos de gestão da organização e discutidos com as partes interessadas apropriadas.

Art. 53. Os tomadores de decisão e outras partes interessadas devem estar cientes da natureza e da extensão do risco residual, após o tratamento do risco.

Art. 54. O risco residual deve ser documentado e submetido a monitoramento, análise crítica e, quando apropriado, a tratamento adicional.

Art. 55. Uma atividade importante nessa etapa é a realização de *workshops* e/ou entrevistas adicionais com gestores e operadores dos processos, com o objetivo de validar os riscos inventariados e indagar a respeito dos controles internos existentes associados a cada risco.

Subseção III
Documentos de tratamento e controle de riscos

Art. 56. Matriz de Tratamento de Riscos.

§ 1º Depois de o risco ter sido identificado, avaliado e mensurado, deve-se definir qual tratamento será atribuído ao mesmo por meio da Matriz de Tratamento de Riscos (Anexo B), a fim de se reduzir a classificação daqueles que são mais críticos.

§ 2º Com base na Matriz de Tratamento de Riscos, serão levantados os controles a serem implementados, visando ao devido tratamento. O resultado desta análise também resultará em

recomendações de melhorias na gestão de riscos, as quais deverão ser inseridas nos Planos de Tratamento de Riscos.

§ 3º A confecção desta matriz possibilitará a visualização de todos os riscos da organização, inclusive de seus diversos setores, principalmente quanto ao tipo de tratamento, a classificação de riscos e seus respectivos gestores.

§ 4º Todos os Comitês e Equipes de Gestão de Riscos e Controles, bem como os programas e projetos, deverão confeccionar esta matriz.

Art. 57. Plano de Tratamento de Riscos.

§ 1º Para os casos de riscos inicialmente classificados como extremos e altos, deve-se sempre elaborar o Plano de Tratamento de Riscos (Anexo C) e realizar nova avaliação (P x I), a fim de se verificar se as ações de controle previstas de serem adotadas realmente reduzem o potencial do risco. Os riscos médios, dependendo do caso, também poderão ser tratados.

§ 2º O Plano de Tratamento de Riscos identificará claramente a ordem de prioridade em que cada tratamento será implementado.

§ 3º Para a elaboração do Plano de Tratamento de Riscos, utilizar-se-á a técnica de resposta às perguntas 5W2H, tendo-se por base os dados da Matriz de Tratamento de Riscos e outras informações relevantes.

§ 4º Cada risco deverá ter o seu respectivo Plano de Contingência, anexo ao Plano de Tratamento de Riscos, que tem o objetivo de reduzir os prejuízos, caso o risco venha a se efetivar, transformando um evento em um problema. Ele não é um comprometimento único ou um projeto com datas de início e término, mas é um processo contínuo de atividades de:

I - treinamento e reciclagem de treinamento de pessoas envolvidas no plano;

II - desenvolvimento e revisão de normas e padrões;

III - exercício de estratégias, procedimentos, equipe e recursos necessários;

IV - pesquisa de processos e tecnologias para melhorar o tempo de resposta e recuperação; e

V - manutenção de atividades pertinentes.

§ 5º O tratamento de riscos, por si só, pode introduzir novos riscos. Um risco significativo pode derivar do fracasso ou da ineficácia das medidas de tratamento de riscos. O monitoramento precisa fazer parte do plano de tratamento de forma a garantir que as medidas permaneçam eficazes.

§ 6º Este tratamento também pode introduzir riscos secundários que necessitam ser avaliados, tratados, monitorados e analisados criticamente. Esses riscos secundários devem, se possível, ser incorporados no mesmo plano de tratamento do risco original e não tratados como um novo risco. Convém que a ligação entre estes riscos seja identificada e preservada.

§ 7º Os indicadores de resultados e de tendências deste plano deverão ser levantados conforme previsto na Portaria nº 214-EME, de 7 de junho de 2016, Manual Técnico (EB20-MT-11.003) Gestão de Indicadores de Desempenho, 1ª Edição, 2016.

§ 8° Todos os Comitês e Equipes de Gestão de Riscos das Organizações Militares, bem como os programas e projetos, deverão ter seus respectivos Planos de Tratamento de Riscos.

Art. 58. Matriz de Riscos e Controles.

§ 1º Após as análises dos Planos de Tratamento de Riscos, passa-se à elaboração da Matriz de Riscos e Controles (Anexo D), para a qual se deverá utilizar os seguintes conceitos:

I - Controle: é uma ação tomada para certificar-se de que algo se cumpra. Os controles também são meios usados para verificar que certa ação é eficiente ao seu propósito. Exemplo: garantia de que as atividades do processo fluam numa sequência lógica;

II - Tipo de controle: manual ou automático (sem intervenção humana);

III - Descritivo do controle: é a descrição da atividade do controle propriamente dita. Exemplo: checar a sequência lógica das atividades previstas no fluxo do processo;

IV - Objetivo do controle: refere-se à existência e/ou necessidade do controle. Exemplo: garantir que toda e qualquer informação inserida no sistema seja íntegra e completa;

V - Periodicidade: refere-se à periodicidade do uso do controle, podendo ser diário, semanal, quinzenal, mensal etc;

VI - Categorias do controle:

a) Preventivo: desenhado para prevenir resultados indesejáveis. Reduzem a possibilidade de sua ocorrência; e

b) Detectivo: desenhado para detectar fatos indesejáveis. Detectam a manifestação/ocorrência de um risco.

VI - Nível de eficácia: refere-se à conceituação da ação de controle, se eficaz ou ineficaz.

§ 2º Após a identificação e associação dos controles aos riscos, os respectivos controles devem ser reavaliados pelos proprietários de riscos e responsáveis pelo processo, podendo ser desenvolvidos e aplicados questionários para coletar a percepção do corpo operacional e gerencial responsável pelo processo no que toca à sua eficácia na mitigação dos riscos.

§ 3º O risco residual estimado representa o resíduo de risco inerente que permanece após aplicação dos controles, ou ainda a parcela do risco carente de controles internos para que seja mitigado por completo. É considerado estimado porque os efeitos dos controles ainda não necessariamente foram aferidos nessa etapa do trabalho, muitas vezes baseando-se em critérios predominantemente qualitativos.

§ 4º Os Comitês e Equipes de Riscos e Controles das Organizações Militares, bem como os programas e projetos, elaborarão esta matriz para os seus processos críticos (que contêm riscos elevados),

conforme Apêndice 1, do Anexo D. Além disso, elaborarão, ainda, esta matriz referente aos riscos dos seus Portfólios de Riscos Prioritários, conforme Apêndice 2, do referido anexo.

Art. 59. Portfólio de Riscos Prioritários.

§ 1º Os 15 riscos mais críticos dos Comitês e Equipes de Gestão de Riscos e Controles das Organizações Militares, bem como dos programas e projetos, serão listados em seus Portfólios de Riscos Prioritários (Anexo E).

§ 2º A confecção desse documento visa a que a organização, inclusive os seus diversos setores, tenham a maior atenção àqueles riscos que, em tese, possuem maior potencial de prejudicar a conquista dos seus objetivos.

§ 3º Estas listas, chamadas de TOP 15, deverão ser revisadas a cada semestre.

Art. 60. Plano de Gestão de Riscos.

§ 1º Os Comitês e Equipes de Gestão de Riscos e Controles das Organizações Militares, bem como os programas e projetos, organizarão seus Planos de Gestão de Riscos (Anexo A) que serão integrados pelos seguintes anexos: Portfólio de Riscos Prioritários; Matriz de Tratamento de Riscos; Planos de Tratamento de Riscos; e Matriz de Riscos e Controles. Quando se tratar do plano da Organização Militar propriamente dita, estes documentos serão assinados pelo seu Comandante, Chefe ou Diretor.

§ 2º Ao Plano de Gestão de Riscos devem, ainda, ser juntados os Relatórios de Monitoramento de Indicadores de Riscos e os Relatórios das Reuniões de Análise da Gestão de Riscos.

§ 3º As Organizações Militares adotarão seus próprios sistemas e modelos de documentos para a confecção destes relatórios, bem como para seu arquivamento e controle.

Seção VI
Monitoramento e análise crítica

Art. 61. O monitoramento e a análise crítica devem ser planejados como parte do processo de gestão de riscos e envolver a checagem ou vigilância regulares. Podem ser periódicos ou acontecer em resposta a um fato específico.

Parágrafo único. As responsabilidades relativas ao monitoramento e à análise crítica devem ser claramente definidas no Plano de Gestão de Riscos.

Art. 62. Os processos de monitoramento e análise crítica da organização devem abarcar todos os aspectos do processo da gestão de riscos, com a finalidade de:

I - obter informações adicionais para melhorar o processo de avaliação dos riscos;

II - analisar os eventos (incluindo os “quase incidentes”), mudanças, tendências, sucessos e fracassos e aprender com eles;

III - detectar mudanças nos contextos externo e interno, incluindo alterações nos critérios de risco e no próprio risco, as quais podem requerer revisão dos tratamentos dos riscos e suas prioridades; e

IV - identificar os riscos emergentes.

Art. 63. Os resultados do monitoramento e da análise crítica devem ser registrados e reportados externa e internamente conforme apropriado, e também convém que sejam utilizados como entrada para a análise crítica da estrutura de gestão de riscos.

Art. 64. As atividades de gestão de riscos devem ser rastreáveis. No processo de gestão de riscos, os registros fornecem os fundamentos para a melhoria dos métodos e ferramentas, bem como de todo o processo.

Art. 65. As decisões relativas à criação de registros devem levar em consideração:

I - a necessidade da organização de aprendizado contínuo;

II - os benefícios da reutilização de informações para fins de gestão;

III - os custos e os esforços envolvidos na criação e manutenção de registros;

IV - as necessidades de registros legais, regulatórios e operacionais;

V - o método de acesso, facilidade de recuperação e meios de armazenamento;

VI - o período de retenção; e

VII - a sensibilidade das informações.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 66. Muitos riscos que não forem incluídos nas matrizes de tratamento de riscos e/ou nos portfólios de riscos prioritários de determinada área, em tese, pelo critério do recobrimento, constarão nos planos de ação dos diversos Comitês e Equipes de Gestão de Riscos subordinadas, responsáveis pelo controle do evento de risco propriamente dito.

Art. 67. Deve-se considerar a documentação a seguir como prevista para as fases do processo de gestão de riscos:

ETAPAS	DOCUMENTOS PREVISTOS
1 - Identificação de riscos	- Estudo do ambiente externo e interno - Matriz de Identificação de Riscos
2 - Análise de riscos	- Matriz de Exposição a Riscos
3 - Avaliação de riscos	- Matriz de Priorização de Riscos
4 - Tratamento de riscos e ações de contingência	- Matriz de Tratamento de Riscos - Planos de Tratamento de Riscos - Portfólio de Riscos Prioritários - Matriz de Riscos e Controles

5 - Comunicação e consulta (ação permanente)	- DIEx ou mensagens (e-mails corporativos) de comunicação de eventos (positivos e negativos) - DIEx ou mensagens (e-mails corporativos) de consulta de providências
6 - Monitoramento e análise crítica (ação permanente)	- Relatório de Monitoramento de Indicadores de Riscos - Relatório das Reuniões de Análise da Gestão de Riscos

Quadro 9 - Lista de documentos produzidos

Art. 68. Para fins de avaliações e auditorias do Escalão Superior e dos Órgãos de Controle Interno e Externo, todos os Comitês e Equipes de Gestão de Riscos e Controles das Organizações Militares inspecionadas deverão ficar em condições de apresentar seus respectivos Planos de Gestão de Riscos.

Art. 69. Todas as Seções e Repartições das Organizações Militares deverão ter permanentemente expostos, em quadros de avisos, os seus respectivos Portfólios de Riscos Prioritários, devidamente atualizados, respeitando-se as regras de sigilo institucionais.

Art. 70. Informações complementares desta Metodologia estarão disponíveis na intranet do Estado-Maior do Exército.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 31000:2009 - Gestão de Riscos: Princípios e Diretrizes.

_______. NBR ISO/TR 31004:2015 - Guia para Implementação da ABNT NBR ISO 31000.

_______. NBR ISO 31010:2009 - Técnicas para o Processo de Avaliação de Riscos.

_______. NBR ISO/IEC 27001:2013 - Segurança da Informação.

CONTROLADORIA GERAL DA UNIÃO E MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. Instrução Normativa Conjunta CGU/MP nº 001, de 10 de maio de 2016 - Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Guia de Orientação para Gestão de Riscos Corporativos. 2007.

MINISTÉRIO DA DEFESA. Exército Brasileiro. Política de Gestão de Riscos do Exército Brasileiro. Brasília, 2017.

_______. Exército Brasileiro. Portaria nº 176-EME, de 29 de agosto de 2013 - Aprova as Normas para Elaboração, Gerenciamento e Acompanhamento de Projetos no Exército Brasileiro (EB20-N-08.001).

_______. Exército Brasileiro. Portaria nº 214-EME, de 7 de junho de 2016 - Aprova o Manual Técnico (EB20-MT-11.003) - Gestão de Indicadores de Desempenho.

_______. Exército Brasileiro. Portaria nº 054-Cmt Ex, de 30 de janeiro de 2017 - Aprova as Normas para Elaboração, Gerenciamento e Acompanhamento do Portfólio e dos Programas Estratégicos do Exército Brasileiro (EB10-N-01.004).

PROJECT MANAGEMENT INSTITUTE (PMI). Guia de Conhecimento sobre Gerenciamento de Projetos (PMBOK, sigla em inglês), 5ª edição, 2015.

TRIBUNAL DE CONTAS DA UNIÃO. Referencial Básico de Governança. Brasília, 2014.

_______. Manual de Critérios Gerais de Controle Interno na Administração Pública. Brasília, 2009.

ANEXO A - PLANO DE GESTÃO DE RISCOS (modelo)
(CABEÇALHO DA OM)

PLANO DE GESTÃO DE RISCOS DA SPE3/3ª SCh EME

1. FINALIDADE

Estabelecer procedimentos para a identificação de eventos capazes de afetar a consecução dos processos da SPE3/3ª SCh EME, bem como administrá-los de modo a mantê-los compatíveis com o apetite a riscos. Além disso, aprimorar os controles internos da gestão e possibilitar garantia razoável ao cumprimento dos objetivos da 3ª Subchefia.

2. REFERÊNCIAS

a. Instrução Normativa Conjunta nº 1 - CGU e MP, de 10 MAIO 16 - dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal;

b. Portaria nº 465, de 17 de maio de 2017 - institui a Política de Gestão de Riscos do Exército Brasileiro (EB10-P-01.004);

c. Portaria nº ____, de __________ - aprova a Diretriz Metodológica da Política de Gestão de Riscos do Exército Brasileiro (EB20-D-07-089);

d. Portaria nº 306-EME, de 22 DEZ 14 - aprova a Sistemática de Planejamento Estratégico do Exército (SIPLEx); e

e. Portaria nº 090-EME, de 12 JUL 10 - aprova o Regimento Interno do EME (RI/R-173).

3. EXECUÇÃO

a. Equipe de Gestão de Riscos e Controles (EGRiC/SPE3)

1) Chefe: Ch SPE3.

2) Membros:

- Ch Subseção de Medição (BSC); e

- Ch Subseção da Supervisão de Gestão de Riscos e Controles.

3) Observação: a EGRiC/SPE3 está subordinada ao Comitê de Gestão de Riscos e Controles da 3ª SCh EME (CGRiC/3ª SCh EME).

b. Atribuições

1) Compete à Equipe de Gestão de Riscos e Controles:

a) elaborar o processo de gestão de riscos da Seção, inclusive o respectivo Plano de Gestão de Riscos;

b) definir os indicadores de desempenho de gerenciamento de riscos que estejam alinhados com os indicadores de desempenho do escalão enquadrante;

c) reunir-se semestralmente para avaliar, revisar e adequar o respectivo processo de gestão de riscos;

d) atualizar semestralmente o Portfólio de Riscos Prioritários da Seção (TOP 15), mas gerenciando todos os demais possíveis riscos por meio dos seus processos;

e) reunir-se anualmente para avaliar, revisar e adequar o Plano de Gestão de Riscos; e

f) supervisionar os trabalhos dos proprietários de riscos.

2) Compete aos proprietários de riscos:

a) assegurar que o risco seja gerenciado de acordo com a Política de Gestão de Riscos do Exército, sua Metodologia e este Plano de Gestão de Riscos;

b) monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados;

c) assegurar a implementação dos planos de ação definidos para tratamento dos riscos sob sua responsabilidade;

d) garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da 3ª Subchefia, considerando o seu respectivo sigilo;

e) operacionalizar os controles internos da gestão; e

f) identificar e comunicar as deficiências de gestão de riscos e de controles internos.

Para fins de responsabilização, destaca-se que os proprietários de riscos respondem civil, penal e administrativamente pelo exercício irregular de suas atribuições.

3) Compete aos demais militares e servidores civis em geral:

a) contribuir nas atividades de identificação e avaliação dos riscos inerentes aos processos de sua responsabilidade;

b) comunicar tempestivamente os riscos inerentes aos seus processos, não mapeados anteriormente; e

c) apoiar os gestores na definição dos planos de ação necessários para tratamento dos riscos.

c. Processos da SPE3

FINALÍSTICOS	FATORES CRÍTICOS DE SUCESSO
Acompanhamento e alinhamento estratégico dos Objetivos Estratégicos do Exército	1 - Informações consistentes do PEEx, gerentes de programas, projetos, ODS, OADI, ODOp, nos prazos estabelecidos
	2 - Planejamento eficaz de curto, médio e longo prazos
	3 - Pessoal capacitado e motivado na realização do Acompanhamento e Alinhamento Estratégico dos OEE
	4 - Existência de ferramenta de TI integradora
	5 - Existência do Sistema de Medição de Desempenho Organizacional (SMDO) nas OM do nível gerencial
GERENCIAIS	FATORES CRÍTICOS DE SUCESSO
Medição e avaliação do desempenho organizacional	1 - Mapa Estratégico do EB, dos ODS, OADI, ODOp elaborados e atualizados
	2 - BSC elaborado no nível estratégico e gerencial
	3 - Coleta de dados, para alimentar o SMDO - EB, realizada oportunamente
	4 - Realização das RAE
Supervisão da gestão de riscos e controles	1 - Cumprimento do calendário de inspeções e controles
	2 - Nível gerencial preparado adequadamente para receber as inspeções
	3 - Existência do modelo de relatório do Plano de Acompanhamento Estratégico

FINALÍSTICOS	FATORES CRÍTICOS DE SUCESSO
	4 - Uso de ferramenta de TI para a gestão de riscos
	5 - Disponibilidade de recursos financeiros para diárias e passagens visando à supervisão da gestão de riscos
DE APOIO/SUPORTE	FATORES CRÍTICOS DE SUCESSO
Efetivação do Ciclo de Capacitação Continuada	1 - Disponibilização de recursos financeiros para a efetivação do Ciclo de Capacitação Continuada
	2 - Contratação de empresas especializadas em capacitação do ciclo de gestão estratégica
	3 - Definição da capacitação a ser realizada
	4 - Escolha criteriosa dos militares a serem capacitados
Registro e controle dos dados de acompanhamento estratégico	1 - Execução do PEEx
	2 - Execução das RAE
	3 - Execução das capacitações em planejamento estratégico, BSC e na plataforma Brainstorming-web
	4 - Execução dos Contratos de Objetivos do Exército (COE)
Planejamento das atividades anuais	1 - Confecção da ordem de serviço regulando as atividades da SPE3
	2 - Elaboração dos planos
	3 - Atualização do SMDO

d. Cronograma de trabalho

OCASIÃO	ATIVIDADES
quinzenal	*Brainstorming* sobre surgimento de novos riscos
mensal	Acompanhamento dos riscos e controles
MAR, JUN, SET e DEZ	Reuniões de Análise da Gestão de Riscos
JUN e DEZ	Atualização da Matriz de Riscos e Controles
JUN e DEZ	Atualização do Portfólio de Riscos Prioritários
MAR, JUN, SET e DEZ	Relatório das Reuniões de Análise da Gestão de Riscos

4. PRESCRIÇÕES DIVERSAS

a. A SPE-3 adotará planilhas impressas para registro de dados, até a implantação do sistema informatizado de gestão de riscos e controles.

b. A gestão dos riscos será realizada de forma individualizada, conforme o Anexo __ - Plano de Tratamento de Riscos.

c. O apetite a riscos da SPE3 está limitado a riscos altos, conforme a definição contida no Art. 39 da Política de Gestão de Riscos do Exército.

d. Os riscos extremos, conforme previsto na Política e na Diretriz Metodológica de Gestão de Riscos só deverão ser aceitos com autorização do Chefe do Estado-Maior do EME.

e. Os riscos que, devido à evolução dos acontecimentos, vierem a atingir os níveis “Alto” e “Extremo” serão sempre avaliados pela CGRiC/3ª SCh EME em Reuniões de Análise da Gestão de Riscos (extraordinárias), para as devidas comunicações e providências emergenciais.

5. ANEXOS

Anexo B - Matriz de Tratamento de Riscos

Anexo C - Plano de Tratamento de Riscos

Anexo D - Matriz de Riscos e Controles

Anexo E - Portfólio de Riscos Prioritários (TOP 15)

Brasília-DF, ___ de maio de 2017

FULANO DE TAL - Cel
Ch SPE3/3ª SCh EME

ANEXO B - MATRIZ DE TRATAMENTO DE RISCOS (modelo)

Aprovada em*:
__/__/__

____
MAJ FULANO
Pres CGRiC

Visto do Rspnl:
__/__/__

____
Cap BELTRANO
Ch EGRiC

DA _______/________ (subordinação)
(__ º semestre de 201__)

O Prio	Código do risco	Objetivos** ou processos	Riscos	Tipo de tratamento	Classificação inicial/final***	Gestor do risco
1º					/	
2º					/	
3º					/	
...					/	
n****					/	

* Quando se referir à Organização Militar propriamente dita, haverá somente o visto do seu Comandante, Chefe ou Diretor. Idem para os demais documentos anexos.
** Objetivos são usados prioritariamente para o planejamento global de Organização Militar.
*** A classificação final será somente registrada após a confecção do respectivo plano de tratamento.
**** Serão listados todos os riscos (de extremos a baixos).

Legenda:
CGRiC: Comitê de Gestão de Riscos e Controles
EGRiC: Equipe de Gestão de Riscos e Controles

ANEXO C - PLANO DE TRATAMENTO DE RISCOS (modelo)

Aprovada em: __/__/__ ___________ MAJ FULANO Pres CGRiC	**DA** _______/________ (subordinação) (__º semestre de 201__) **Apêndice 1 - RISCO (código):** ___(identificação do risco)______ Gestor do risco (posto ou Grad e nome): ____________________	Visto do Rspnl: __/__/__ ___________ Cap BELTRANO Ch EGRiC

Classificação inicial: ________________			Resposta ao risco: __ _(tipo de tratamento a ser realizado)__			
P x I (com as Mdd tratamento): __x __ = __			Classificação final: ___________________			
O QUÊ?	QUEM?	QUANDO?	ONDE?	POR QUE?	COMO?	CUSTO?
1.						
...						
n						

MONITORAMENTO DO RISCO RESIDUAL															
INDICADORES	TIPO*	FÓRMULAS	METAS	MEDIÇÕES REGULARES											
				J	F	M	A	M	J	J	A	S	O	N	D

* resultado e tendências (conforme o Manual Técnico EB20-MT-11.003)

REGISTRO DE OCORRÊNCIAS			
DATA	MEDIÇÃO CRÍTICA	DESCRIÇÃO SUMÁRIA	Doc QUE COMUNICOU (sfc)

ANEXO - PLANO DE CONTINGÊNCIA

HIPÓTESE 1: (Se ocorrer a situação X)_______________________________________

O QUÊ?	QUEM?	QUANDO?	ONDE?	POR QUE?	COMO?	CUSTO?
1.						
....						
n						

Treinamentos e avaliações

DATA	AVALIAÇÃO*	AVALIADOR	OBSERVAÇÕES**
__/___/___			
...			
MÉDIA		-	-

* Menções globais (I - 0; R - 3; B - 5; MB - 8; 10 - E)

** Boletim Interno que publicou o resultado do treinamento da Organização Militar e/ou outras informações (favoráveis e/ou desfavoráveis - Art. 57)

HIPÓTESE 2: (Se ocorrer a situação Y)_______________________________________

O QUÊ?	QUEM?	QUANDO?	ONDE?	POR QUE?	COMO?	CUSTO?
1.						
....						
n						

Treinamentos e avaliações

DATA	AVALIAÇÃO*	AVALIADOR	OBSERVAÇÕES**
__/___/___			
...			
MÉDIA		-	-

* Idem ** Idem

Local e data

____
Nome - posto ou graduação
Gestor do risco

MENÇÕES GLOBAIS*

CUMPRIMENTO DOS REQUISITOS	MENÇÃO	VALOR
acima de 90%	E	10
entre 70% e abaixo de 90%	MB	8
entre 50% e abaixo de 70%	B	5
entre 20% e abaixo de 50%	R	3
abaixo de 20%	I	0

Apêndice 2 - RISCO (código): ___(identificação do risco)_________
Gestor do risco (Posto/Grad e nome): ___________________________
....

Apêndice "n" - RISCO (código): ___(identificação do risco)________
Gestor do risco (Posto/Grad e nome): ___________________________
....

Aprovada em:		Visto do Rspnl:
__/__/__		__/__/__
____________		____________
MAJ FULANO		Cap BELTRANO
Pres CGRiC		Ch EGRiC

ANEXO D - MATRIZ DE RISCOS E CONTROLES
Apêndice 1 - PROCESSOS CRÍTICOS

PROCESSO 1: aquisição de bens e serviços

Dados do Risco							Avaliação do risco inerente			Atividades de controle do risco (tratamento)						Avaliação do controle (estimativa)				
Código do risco (O Prio)	Objetivo do processo	Risco inerente ao processo	Causa potencial	Fonte da causa	Vulnerabilidade da causa	Conse-quência potencial	P	I	Resultado (P x I) e classificação do risco	Código do controle	Controle	Tipo de controle	Descrição	Objetivo do controle	Periodi cidade	Nível de eficácia	Categoria	P	I	Resultado (P x I) e classificação do risco residual
R1	**Atender uma necessidade da organização com produtos e serviços**	**Não atender aos requisitos**	**Requisição confeccio-nada por quem não necessita-do produto e/ou serviço**	Processos	Fluxo do processo mal concebido	**Não aquisição de produto e/ou serviço**	**5**	**1**	**5 (MÉDIO)**	C1	Garantir que as atividades do processo fluam numa sequência lógica	Manual	Checar a sequência lógica das atividades previstas no fluxo do processo	Integridade das informações	Mensal	Eficaz	Preventivo	**2**	**1**	**2 (BAIXO)**
					Ausência de procedimentos formalizados					C2	Garantir que todos os procedimentos estejam formalizados em documentos específicos	Manual	Checar se os procedimentos executados estão previstos em documento específico	Conformidade com leis e regulamentos	Mensal	Eficaz	Preventivo			
				Estrutura organizacio-nal	Falta de clareza quanto às funções e responsabilida-des					C3	Garantir que as funções e responsabilidades estejam bem definidas	Manual	Checar a responsabilidade pela execução da atividade	Conformidade com leis e regulamentos	Mensal	Eficaz	Preventivo			
					Delegações exorbitantes					C4	Garantir que não haja delegações exorbitantes	Manual	Checar se a competência delegada não extrapola as atribuições definidas	Conformidade com leis e regulamentos	Mensal	Eficaz	Preventivo			
R2																				
R3																				
R4																				
R?																				
Nível de risco inerente: _______________* *Somatório dos resultados de P x I : Nr de riscos									Soma*:	-	-	-	-	-	-	Nível de risco residual: __________* *Somatório dos resultados de P x I : Nr de riscos				Soma*:

PROCESSO 2: _______________________________

PROCESSO "n": _______________________________

Escala do nível de risco do processo:
Baixo: de 1 a 2,99
Médio: de 3 a 7,99
Alto: de 8 a 14,99
Extremo: de 15 a 25

Aprovada em:
__/__/__

____
MAJ FULANO
Pres CGRiC

ANEXO D - MATRIZ DE RISCOS E CONTROLES
Apêndice 2 - PORTFÓLIO DE RISCOS PRIORITÁRIOS (TOP 15)

Visto do Rspnl:
__/__/__

____
Cap BELTRANO
Ch EGRiC

Dados do Risco						Avaliação do risco inerente			Atividades de controle do risco (tratamento)						Avaliação do controle (estimativa)				
Código do risco (O Prio)	Risco inerente	Causa potencial	Fonte da causa	Vulnerabilidade da causa	Consequência potencial	P	I	Resultado (P x I) e classificação do risco	Código do controle	Controle	Tipo de controle	Descrição	Objetivo do controle	Periodicidade	Nível de eficácia	Categoria	P	I	Resultado (P x I) e classificação do risco residual
R1																			
R2																			
R3																			
R4																			
..																			
..																			
R15																			
Nível de risco inerente: ___________* *Somatório dos resultados de P x I : Nr de riscos								Soma:	-	-	-	-	-	-	Nível de risco residual: ___________* *Somatório dos resultados de P x I : Nr de riscos				Soma:

Escala do nível de risco do portfólio:
Baixo: de 1 a 2,99
Médio: de 3 a 7,99
Alto: de 8 a 14,99
Extremo: de 15 a 25

Aprovada em:
__/__/__

____
MAJ FULANO
Pres CGRiC

ANEXO E - PORTFÓLIO DE RISCOS PRIORITÁRIOS (TOP 15) (modelo)

DA _______/________ (subordinação)

(__º semestre de 201_)

Visto do Rspnl:
__/__/__

____
Cap BELTRANO
Ch EGRiC

O Prio	Código do risco	Objetivos ou processos	Riscos	Classificação final de risco	Gestor do risco
1º					
2º					
3º					
4º					
5º					
6º					
7º					
8º					
9º					
10º					
11º					
12º					
13º					
14°					
15º					